



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/668,112	09/22/2000	Michael L. Grandcolas	CITI0185	9577
27510	7590	11/17/2004	EXAMINER	
KILPATRICK STOCKTON LLP 607 14TH STREET, N.W. WASHINGTON, DC 20005			PARTHASARATHY, PRAMILA	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 11/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/668,112

Applicant(s)

GRANDCOLAS ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 June 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 and 25-43 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 and 25 - 43 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in response to request for reconsideration filed on June 30, 2004. Original application contained Claims 1 – 48. Applicant has amended Claims 1, 15, 18, 25, 39 and 42. Claims were 20 – 24 and 44 – 48 were canceled. Therefore, presently pending claims are 1 – 19 and 25 – 43.

Response to Arguments

2. Applicant's arguments filed on June 30, 2004, have been fully considered but they are not persuasive for the following reasons:

Regarding independent amended claims 1 and 25, applicant argued that the cited prior art (CPA) [Sasmazel et al. U.S. Patent 6,263,432] does not teach, "determining a second web server related to the user's request by a first web server and in response thereto creating an encrypted authentication token related to the user and redirecting the user's web browser to the second web server by the first web server" and "transmitting the encrypted authentication token from the first web server to a second web server via the user's web browser and authenticating the authentication token and allowing the user to conduct a session at the second web server". These arguments are not found persuasive. Sasmazel clearly teaches and applicant agrees (see page 14 of Remarks/Arguments) authenticating a user by an authentication server

after receiving a user's request and applicant also agrees that the ticket includes the user's authentication and authorization information. Sasmazel discloses authenticating a user at a first web server (Column 2 lines 19 - 59 and Column 7 line 39 – Column 8 line 55); detecting a client request at said first web server, said first web server determining a second web server related to the request and in response thereto creating an encrypted authentication token related to the user and redirecting a web browser of the user to the second web server (Column 2 lines 19 – 59; Column 6 line 10 – 39; and Column 10 lines 9 – 50); transmitting the encrypted token from the first web server to the second web server via the user's web browser, wherein the authentication token comprises an expiration time and is digitally signed by the first web server (Column 2 lines 19 – 64 and Column 7 lines 18 – 67); authenticating the authentication token at the second web server (Column 2 lines 19 – 64 and Column 8 line 1 – Column 9 line 28); and allowing the user to conduct a session at the second web server (Column 9 lines 10 – 33).

Applicant has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that CPA does teach or suggest the subject matter broadly recited in independent claims 1 and 25. Dependent claims 2 – 19 and 26 - 43 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 1 – 19 and 25 - 43 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

3. Claims 1- 48 are rejected under 35 U.S.C. 102(e) as being anticipated by Sasmazel et al. (U.S. Patent No.: 6,263,432).

Regarding Claim 1, Sasmazel teaches and describes, a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), comprising:

authenticating a user at a first web server (Column 2 lines 19 - 59 and Column 7 line 39 – Column 8 line 55);

detecting a client request at said first web server, said first web server determining a second web server related to the request and in response thereto creating an encrypted authentication token related to the user and redirecting a web browser of the user to the second web server (Column 2 lines 19 – 59; Column 6 line 10 – 39; and Column 10 lines 9 – 50);

transmitting the encrypted token from the first web server to the second web server via the user's web browser, wherein the authentication token comprises an expiration time and is digitally signed by the first web server (Column 2 lines 19 – 64 and Column 7 lines 18 – 67);

authenticating the authentication token at the second web server (Column 2 lines 19 – 64 and Column 8 line 1 – Column 9 line 28); and

allowing the user to conduct a session at the second web server (Column 9 lines 10 – 33).

Regarding Claim 25, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), comprising:

a means for authenticating a user at a first web server (Column 2 lines 19 - 59 and Column 7 line 39 – Column 8 line 55);

means for detecting a client request at said first web server, said first web server determining a second web server related to the request and in response thereto creating an encrypted authentication token related to the user and redirecting a web browser of the user to the second web server (Column 2 lines 19 – 59; Column 6 line 10 – 39; and Column 10 lines 9 – 50);

a means for transmitting the encrypted token from the first web server to the second web server via the user's web browser, wherein the authentication token

comprises an expiration time and is digitally signed by the first web server (Column 2 lines 19 – 64 and Column 7 lines 18 – 67);

a means for authenticating the authentication token at the second web server (Column 2 lines 19 – 64 and Column 8 line 1 – Column 9 line 28); and

a means for allowing the user to conduct a session at the second web server (Column 9 lines 10 – 33).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the first web server and the second web server share a sub-domain (Fig. 2 #220, #240 and Column 6 lines 10 – 40 and Column 10 lines 10 – 30).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the first web server and the second web server share a sub-domain (Fig. 2 #220, #240 and Column 6 lines 10 – 40 and Column 10 lines 10 – 30).

Claim 39 is rejected as applied above in rejecting claim 25. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to a

federation of web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising:

a means for sending the digitally signed authentication token to the web browser of the computing device by the first web server (Column 7 lines 39 – Column 8 lines 58); and

a means for sending the authentication token to the second web server by the web browser (Fig. 7 and Column 8 lines 57 – Column 9 line 9).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising examining the expiration time of the authentication token at the second web server and allowing the user to conduct a session at the second web server only if the expiration time has not passed (Fig. 3 #302 and Column 9 lines 10 – 32).

Claim 27 is rejected as applied above in rejecting claim 26. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising a means for examining the expiration time of the authentication token at the second web server (Column Fig. 3 #302; Column 7 lines 45 – 47 and Column 9 lines 10 – 17).

Claim 40 is rejected as applied above in rejecting claim 39. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to a federation of web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising a means for allowing the user to conduct a session with the first web server (Fig. 2 #220 and Column 6 lines 10 – Column 9 line 15).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the authentication token comprises a cookie (Column 6 lines 10 – 57).

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the authentication token comprises a cookie (Column 6 lines 10 – 57).

Claim 41 is rejected as applied above in rejecting claim 40. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to a federation of web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the second web server shares a sub-domain with the first web server (Fig. 2 #220, #240 and Column 6 lines 10 – 40 and Column 10 lines 10 – 30).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein transmitting the encrypted authentication token from the first web server to the second web server comprises transmitting the encrypted authentication token from the first web server to the user, and then from the user to the second web server (Column 8 lines 42 – 58).

Claim 29 is rejected as applied above in rejecting claim 28. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the means for transmitting the encrypted authentication token from the first web server to the second web server comprises means for transmitting the encrypted authentication token from the first web server to the user, and then from the user to the second web server (Column 8 lines 42 – 58).

Claim 42 is rejected as applied above in rejecting claim 41. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to a federation of web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising means for digitally signing the authentication token using public key encryption (Fig. 3 #306 Column 7 lines 18 – 54).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein authenticating the user at the first web server comprises receiving a user name and password (Fig. 6 and Column 8 lines 1 – 5).

Claim 30 is rejected as applied above in rejecting claim 29. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the means for authenticating the user at the first web server comprises receiving a user name and password (Fig. 6 and Column 8 lines 1 – 5).

Claim 43 is rejected as applied above in rejecting claim 42. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to a federation of web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising a means for confirming a match with the digital signature (Fig. 13, Column 6 lines 44 – Column 9 line 28).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein transmitting the encrypted authentication token from the first web server to a second web server comprises transmitting the authentication token from the first web server to a computer of the user; and

transmitting the authentication token from the computer of the user of the second web server (Column 8 lines 42 – 58).

Claim 31 is rejected as applied above in rejecting claim 30. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein transmitting the encrypted authentication token from the first web server to a second web server comprises means for transmitting the authentication token from the first web server to a computer of the user; and means for transmitting the authentication token from the computer of the user of the second web server (Column 8 lines 42 – 58).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the first web server and the second web server comprise a federation of web servers (Column 6 lines 10 – 40, Column 8 lines 46 – 50 and Column 10 lines 40 – 50).

Claim 32 is rejected as applied above in rejecting claim 31. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the first web server and the second web server comprise a federation of web servers (Column 6 lines 10 – 40, Column 8 lines 46 – 50 and Column 10 lines 40 – 50).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein authenticating the authentication token at the second web server comprises examining the cookie (Column 8 lines 46 – 60 and Column 9 lines 10 – 15).

Claim 33 is rejected as applied above in rejecting claim 32. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the means for authenticating the authentication token at the second web server comprises means for examining the cookie (Column 8 lines 46 – 60 and Column 9 lines 10 – 15).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising URL encoding the authentication token (Column 6 lines 10 – 23 and Column 7 lines 38 – 67).

Claim 34 is rejected as applied above in rejecting claim 33. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising a means for URL encoding the authentication token (Column 6 lines 10 – 23 and Column 7 lines 38 – 67).

Claim 11 is rejected as applied above in rejecting claim 10. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising URL decoding the authentication token at the second web server (column 9 lines 10 – 32).

Claim 35 is rejected as applied above in rejecting claim 34. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising a means for URL decoding the authentication token at the second web server (column 9 lines 10 – 32).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising providing a web page to the user having a service selector (Column 6 lines 10 – 40).

Claim 36 is rejected as applied above in rejecting claim 35. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), further comprising providing a web page to the user having a service selector (Column 6 lines 10 – 40).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the service selector comprises a hyperlink (Fig. 7 and Column 6 lines 10 - 23).

Claim 37 is rejected as applied above in rejecting claim 36. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the service selector comprises a hyperlink (Fig. 7 and Column 6 lines 10 - 23).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Sasmazel teaches and describes a method of single sign-on user access to multiple web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the hyperlink comprises a URL for the second web server (Column 6 lines 10 – 40).

Claim 38 is rejected as applied above in rejecting claim 37. Furthermore, Sasmazel teaches and describes, a system for single sign-on user access to multiple web servers (Fig. 7 and Column 4 lines 15 – Column 10 line 40), wherein the hyperlink comprises a URL for the second web server (Column 6 lines 10 – 40).

Claim 15 is rejected as applied above in rejecting claim 7. Furthermore, Sasmazel teaches and describes, a method for single sign-on user access to a federation of web servers (Fig. 7 and Column 10 lines 10 – 30), comprising:

 sending the digitally signed authentication token to the web browser of the computing device by the first web server (Column 7 lines 39 – Column 8 line 58); and

 sending the authentication token to the second web server by the web browser (Fig. 7 and Column 8 lines 57 – Column 9 line 9).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Sasmazel teaches and describes, a method for single sign-on user access to a federation of web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising allowing the user to conduct a session with the first web server (Fig. 2 #220 and Column 6 lines 10 – Column 9 line 15).

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Sasmazel teaches and describes, a method for single sign-on user access to a federation of web servers (Fig. 7 and Column 10 lines 10 – 30), wherein the second web server shares a sub-domain with the first web server (Fig. 2 #220, #240 and Column 6 lines 10 – 40 and Column 10 lines 10 – 30).

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Sasmazel teaches and describes, a method for single sign-on user access to a

federation of web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising digitally signing the authentication token using public key encryption (Fig. 3 #306 Column 7 lines 18 – 54).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Sasmazel teaches and describes, a method for single sign-on user access to a federation of web servers (Fig. 7 and Column 10 lines 10 – 30), further comprising confirming a match with the digital signature (Fig. 13, Column 6 lines 44 – Column 9 line 28).

Conclusion

4. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2136

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
November 09, 2004.


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
EBC CENTER 2100